KEEPER | Pressemitteilung

Keeper Security stellt JetBrains-Erweiterung vor und integriert Zero-Trust-Secrets-Management direkt in Entwickler-Workflows

Neue Integration bringt Secrets-Schutz auf Enterprise-Niveau in JetBrains IDEs, eliminiert hartkodierte Zugangsdaten und sichert die Software-Lieferkette von innen heraus ab.

MÜNCHEN – 7. Januar 2026 – Keeper Security, ein führender Anbieter von Zero-Trust- und Zero-Knowledge-Cybersicherheitssoftware zum Schutz von Passwörtern und Passkeys, Infrastruktur-Secrets, Remote-Verbindungen und Endpunkten, gibt heute den Launch seiner JetBrains-Erweiterung bekannt. Diese bietet Nutzern von JetBrains Integrated Development Environments (IDEs) eine sichere und nahtlose Möglichkeit, geheime Informationen direkt innerhalb ihrer Entwicklungs-Workflows zu verwalten. Durch die direkte Integration mit dem Keeper Vault können Entwickler hartkodierte Geheimnisse durch Vault-Referenzen ersetzen und Befehle mit injizierten Zugangsdaten ausführen, sodass sensible Informationen in jeder Phase der Entwicklung geschützt bleiben.

Sicheres Secrets-Management schützt die Zugangsdaten, API-Schlüssel, Tokens und Zertifikate, auf die Anwendungen für einen sicheren Betrieb angewiesen sind. Werden diese Secrets falsch gehandhabt – etwa indem sie im Klartext gespeichert, im Quellcode hartkodiert oder unsicher geteilt werden –, werden sie zu leichten Zielen für Angreifer. Die Keeper-JetBrains-Erweiterung eliminiert diese Risiken, indem Entwickler geheime Informationen aus dem Keeper Vault speichern, abrufen und generieren können, ohne ihre IDE zu verlassen.

Im Gegensatz zu eigenständigen Plug-ins oder externen Vault-Tools, die auf Drittanbieter-Server angewiesen sind, arbeitet die JetBrains-Erweiterung von Keeper innerhalb einer Zero-Knowledge-Architektur, bei der sämtliche Ver- und Entschlüsselung lokal auf dem Gerät des Nutzers erfolgt. Nativ integriert mit Keeper Secrets Manager und KeeperPAM®, bringt sie Kontrolle für Privilegien auf Enterprise-Niveau direkt in den Entwickler-Workflow und bietet starke Sicherheit, ohne die Entwicklung zu verlangsamen.

„Moderne Softwareentwicklung erfordert Sicherheit auf jeder Ebene“, sagt Craig Lurey, CTO und Mitgründer von Keeper Security. „Die Integration von Keeper in JetBrains stellt sicher, dass Entwickler Secure-by-Design-Prinzipien von Anfang an umsetzen können, hartkodierte Zugangsdaten eliminieren und die Integrität der Software-Lieferkette stärken.“

Zu den wichtigsten Funktionen der Keeper-JetBrains-Erweiterung gehören:

- **Secrets Management:** Speichern, Abrufen und Generieren von Secrets direkt aus dem Keeper Vault.
- **Sichere Befehlsausführung:** Ausführen von Anwendungen mit sicher aus dem Keeper Vault injizierten Secrets.
- **Logging- und Debug-Tools:** Anzeige von Logs und Aktivierung des Debug-Modus für vollständige operative Transparenz.
- **Plattformübergreifende Unterstützung:** Verfügbar für Windows-, macOS- und Linux-Umgebungen.

Die JetBrains-Erweiterung baut auf Keepers umfassender KeeperPAM®-Plattform auf, einer KI-gestützten, cloud-nativen Lösung für Privileged Access Management, die Passwort-, Secrets-, Verbindungs- und Endpunktmanagement unter einem Zero-Trust- und Zero-Knowledge-Framework vereint. KeeperPAM erzwingt Least-Privilege-Zugriffe, ermöglicht automatisierte Credential-Rotation und bietet zentralisierte Transparenz über alle Nutzer und Geräte hinweg, wodurch Organisationen ihre Sicherheit stärken und Compliance vereinfachen können.

Entwickler können die Keeper-JetBrains-Erweiterung direkt in ihrer IDE installieren oder mehr unter docs.keeper.io erfahren.

###

Über Keeper Security:
Keeper Security ist eines der am schnellsten wachsenden Unternehmen für Cybersicherheitssoftware, das Tausende von Organisationen und Millionen von Menschen in über 150 Ländern schützt. Keeper ist ein Pionier der Zero-Knowledge- und Zero-Trust-Sicherheit für jede IT-Umgebung. Das Herzstück, KeeperPAM®, ist eine KI-fähige, Cloud-native Plattform, die alle Benutzer, Geräte und Infrastrukturen vor Cyberangriffen schützt. Keeper wurde für seine Innovationen im Gartner Magic Quadrant für Privileged Access Management (PAM) ausgezeichnet und sichert Passwörter und Passkeys, Infrastrukturgeheimnisse, Remote-Verbindungen und Endpunkte mit rollenbasierten Durchsetzungsrichtlinien, Least-Privilege und Just-in-Time-Zugriff. Erfahren Sie auf KeeperSecurity.com, wie Keeper Ihr Unternehmen vor den heutigen Cyberbedrohungen schützen kann.

Folgen Sie Keeper auf Facebook Instagram LinkedIn X YouTube TikTok

Pressekontakt für Keeper in DACH:
Alexandra Schmidt, +49 170 387 10 64
Thilo Christ, +49 171 622 06 10
keeper@tc-communications.de